UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/591,034	06/09/2000	Chris Rygaard	AdAst-991100	2586

26379 7590 06/16/2004

GRAY CARY WARE & FREIDENRICH LLP
2000 UNIVERSITY AVENUE
E. PALO ALTO, CA 94303-2248

EXAMINER	
JACKSON, JENISE E	

ART UNIT	PAPER NUMBER
2131	10

DATE MAILED: 06/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/591,034	RYGAARD, CHRIS	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-19 rejected under 35 U.S.C. 102(a) as being anticipated by Jansen et al. NIST Special Publication 800-19 – Mobile Agent Security (hereafter Jansen).

2. As per claims 1, 5, 7, Jansen teaches a mobile application security system(see pg. 2, 2nd paragraph, fig. 1), a central computer connected to a server computer, each host computer executing the mobile application that jumps between the hosts during execution, and the central computer including means for monitoring the security of the mobile application as it jumps between the hosts computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer(pg. 13-14, protecting the agents platform section, teaches a "reference monitor" that cannot be bypassed and pg. 18-19, teach central or distributed architecture), are disclosed in Jansen because, Jansen discloses a central host connected to each node for controlling the security of mobile applications/agents(see pg. 18-19 protecting agents section, teaches both central and decentralized server architectures). Further, Jansen teaches a security monitoring means further includes detecting unwanted changes in the code associated with the mobile application when the mobile application is jumping between hosts(see pg. 6-7, section 2.3.4, pg. 9-10, section 3.2, pg. 10-11, section 3.3).

3. As per claim 2, Jansen teaches claim 1/1 wherein the detecting means further comprises means for storing a copy of each MA(mobile application) when the MA is created by having the creating node send a copy of the MA to the Central host, means for receiving data about the MA when it is received by another node and means for comparing the code of the MA received by the other node to the stored copy of the MA to determine if changes have been mode to the code of the MA (Section 3.2, page 9, 1st paragraph teaches protecting against modification of code, i.e. comparing the original to the one received AND section 4.2.2 Mutual Itinerary Recording teaches tracking and comparing the Itinerary list as it traverses the peers – Since Jansen discloses both central and distributed Central host (see claim 1 above), this reads on using one stored copy for comparison purposes. Further to this point are the lists/tables, bottom list on page 14 and top list on page 19, which disclose many possible countermeasure means – one skilled in the art would provide for a one-to-one code compare at a minimum).

4. As per claim 3, Jansen teaches security monitoring means comprises preventing a node from transmitting hostile code in a MA to another node (page 3, Denial of Service section 2.1.2, teaches "malicious code" being introduced by an outside person or by an internal test engineer, etc. AND page 19, top paragraph teaches IBM Aglets prevent receiving platform from accepting agents from an agent platform not defined as a trusted peer, see also, pg. 6-7, section 2.3.4).

5. As per claim 4, Jansen teaches wherein preventing means comprises determining if the node dispatching the mobile application is trusted (pages 18-19, Protecting Agents, teaches trusted peers via IBM Aglets and Claim 3 above teaches Signed Code which infers trust), means for saving the code of the MA and means, when requested by another node, for providing the code for the MA to the requesting node (page 13-14, Protecting Agent Platform section – broadly

discloses "trusted communications for MA's" which inherently includes requesting of MA and transmission of MA) **but is silent on** means for stripping the code from an initially received MA if the host is not trusted.

Jansen teaches identifying a non-trusted machine (see previous claim rejections) and hence many options exist as to how to stay safe from said machine, i.e. do not communicate with it, only transmit to it, attempt to re-verify that it is a trusted machine, only communicate with certain machines, strip code. The examiner believes that stripping code is the most harsh of the possibilities since it may be that a network error occurred or the user entered a bad login/password/certificate/etc., which resulted in the failed trusting operation. The stripping of code should be left to a system administrator.

6. As per claim 6, Jansen teaches wherein the detecting means further comprises means for saving a copy of the state of a MA received from a node that received the MA, means for receiving data about the same MA after a jump to another node and means for comparing the state of the MA after the jump to another node with the stored state of the MA to ensure that the state of the MA has not changed (page 17, section 4.1.4, State Appraisal section).

7. As per claim 8, Jansen teaches wherein the detecting means further comprises means for saving a copy of the itinerary of a MA received from a node that received the MA, means for receiving the same MA after a jump to another node and means for comparing the itinerary of the MA after the jump to another node with the stored itinerary of the MA to ensure that the itinerary of the MA has not changed (page 21-22, section 4.2.2, 4.2.3, Mutual Itinerary Recording and Itinerary Recording with Replication/Voting sections).

8. As per claim 9, Jansen teaches wherein the itinerary comprises past historical itinerary data (page 17, Path Histories section AND page 21, Mutual Itinerary Recording and Itinerary Recording with Replication/Voting sections).

9. As per claim 10, Jansen teaches security monitoring means comprises detecting unwanted changes in the state of the MA (page 17, State Appraisal teaches prevention of state corruption/modification, pg. 18-19).

10. As per claim 12, it is rejected under the same basis as claim 3.

11. As per claim 13, it is rejected under the same basis as claim 4.

12. As per claim 14, Jansen teaches detecting unwanted changes to the itinerary of the MA (page 21, Section 4.2.2, Mutual Itinerary Recording teaches tracking of an agent's itinerary).

13. As per claim 15, limitations have already been addressed(see claim 6).

14. As per claim 16, rejected under the same basis as claim 14.

15. As per claim 17, it is rejected under the same basis as claim 8.

16. As per claim 18, it is rejected under the same basis as claim 9.

17. As per claim 19, Jansen teaches receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host(see pg. 18-19); and monitoring the security of the mobile application as it jumps between the host computers, wherein the security monitoring includes preventing untrusted hosts from initially launching mobile applications(pg. 3, 6-7).

Response to Amendment

18. The Applicant states that Jansen does not disclose the central computer including means for monitoring the security of the mobile application as it jumps between the host computer wherein the mobile application is communicated from the first host to a second host. The Examiner disagrees with the Applicant, Jansen teaches that the Jumping beans agent system addresses security issues by implementing a client-server architecture, whereby an agent always returns to a secure central host before moving onto any other platform(see pg. 19).

19. The Applicant states that Jansen does not disclose the security monitoring means for detecting unwanted changes in the code associated with the mobile application when the mobile application is jumping between hosts. The Examiner disagrees since Jansen teaches a central host allowing tampering to be detected and prevented from accepting agents/code from someone not defined as a trusted peer(see pg. 19).

20. The Applicant states that Jansen does not disclose the central computer detects unwanted changes in the code associated with the mobile application when the mobile application is jumping between hosts. The Examiner disagrees since Jansen teaches a secure central host which is interpreted as being capable of providing central security(see pg. 19). Further, Jansen discloses that a digital signature is included into the code, if the digital signature can verified than the agent has not been tampered with, if it cannot be verified that it has been tampered with(see pg. 16, 18).

21. The Applicant states that Jansen does not teach that a central computer stores a copy of a mobile application and then compares it to the mobile application after execution by another host. The Examiner disagrees with the Applicant. Jansen teaches this, because Jansen teaches protecting against modification of code, i.e. comparing the original to the one received and section 4.2.2 Mutual Itinerary Recording teaches tracking and comparing the Itinerary list as it traverses the peers-Since Jansen teaches both central and distributed Central host(see pg. 19), this reads on using one stored copy for comparison purposes.

22. The Applicant states that Jansen does not disclose means for stripping the code from an initially received mobile application if the host is not trusted, means for saving the code when requested by another host, and for providing the code for the mobile application to the requesting host. The Examiner disagrees with the Applicant. Jansen teaches identifying a non-trusted machine and many options exist as to how to stay safe from the machine. Jansen teaches that one of the options that exist is to only communicate with certain machines, stripping the code(see pg. 13-14).

Final Action

23. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-0040 for regular communications and (703) 308-6306 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

***

June 10, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100